CONCERNING SETS OF POLYNOMIALS ORTHOGONAL SIMULTANEOUSLY ON SEVERAL CIRCLES

G. SZEGÖ

Introduction. Sets of polynomials $\{p_n(z)\}$ simultaneously orthogonal on several curves have been investigated by J. L. Walsh and the author. Recently, the particular case of circles has been treated by G. M. Merriman,* and it is the purpose of this note to give a shorter derivation of his result.

For $r \geqq 0$, $m \geqq 1$ the polynomials

$$1, z, z^2, \cdots, z^{m-1}; \quad z^{n-m}(z^m - r^m), \qquad n = m, m+1, \cdots, \tag{1}$$

are orthogonal on the circles $|z| = R > r$ with the weight function

$$w(z) = |z^m - r^m|^{-2}. \tag{2}$$

From the work of Walsh and the author† we know that if a set of polynomials is orthogonal on two distinct circles, these circles must be concentric, and a very simple relation holds between the corresponding weight functions. According to the results of the author, the case (1), (2) is the only one, save for integral linear transformations, in which a set of polynomials is simultaneously orthogonal on all circles concentric to a given circle and containing it. Merriman shows that this holds true if only the simultaneous orthogonality on two (necessarily concentric) circles is assumed.

Preliminary remarks. In order to prove this pretty result, we shall use the following simple identity satisfied by the polynomials

$$p_n(z) = k_n z^n + \cdots, \qquad k_n > 0; \; n = 0, 1, 2, \cdots, \tag{3}$$

which constitute an orthonormal set on the unit circle $|z| = 1$ with a preassigned weight function $w(t) = w(e^{i\theta}) = f(\theta)$:

$$\sum_{\nu=0}^{n} \overline{p_\nu(0)} p_\nu(z) = k_n z^n \bar{p}_n(z^{-1}). \tag{4}$$

The reader may find this identity in my earlier paper, *Beiträge zur Theorie der Toeplitzschen Formen*, II (Mathematische Zeitschrift, vol. 9 (1921), pp. 167–190, in particular, p. 174, (33)). For the sake of completeness, however, I include here a very simple direct proof for it.

* See a note of the same title as the present one in this Bulletin, vol. 44 (1938), pp. 57–69. Here also references can be found to the literature on the subject.

† Cf. loc. cit.

We conclude from elementary properties of orthogonal functions that $k_n^{-1}p_n(z)$ gives the minimum value of the integral

$$\frac{1}{2\pi}\int_{-\pi}^{+\pi} f(\theta)\,|\,p(z)\,|^2 d\theta, \qquad z = e^{i\theta}, \tag{5}$$

considering the set of all polynomials $p(z)=z^n+\cdots$ of degree n with the highest term z^n. Next, writing

$$z^n\bar{p}(z^{-1}) = u_0p_0(z) + u_1p_1(z) + \cdots + u_np_n(z), \tag{6}$$

we find that this polynomial (6) has the constant term 1 if $p(z)$ has the highest term z^n, so that

$$u_0p_0(0) + u_1p_1(0) + \cdots + u_np_n(0) = 1.$$

Now, according to Cauchy's inequality,

$$\begin{aligned} 1 &= \left|\sum_{\nu=0}^{n} u_\nu p_\nu(0)\right|^2 \leqq \sum_{\nu=0}^{n}|\,u_\nu\,|^2 \sum_{\nu=0}^{n}|\,p_\nu(0)\,|^2 \\ &= \sum_{\nu=0}^{n}|\,p_\nu(0)\,|^2 \frac{1}{2\pi}\int_{-\pi}^{+\pi} f(\theta)\,|\,z^n\bar{p}(z^{-1})\,|^2 d\theta \\ &= \sum_{\nu=0}^{n}|\,p_\nu(0)\,|^2 \frac{1}{2\pi}\int_{-\pi}^{+\pi} f(\theta)\,|\,p(z)\,|^2 d\theta, \qquad z = e^{i\theta}, \end{aligned}$$

with the equality sign being taken if and only if

$$u_\nu = \overline{p_\nu(0)}\left\{\sum_{\nu=0}^{n}|\,p_\nu(0)\,|^2\right\}^{-1}, \quad \nu = 0, 1, 2, \cdots, n.$$

Therefore, save for a constant factor, (4) follows. This factor may be determined by comparing the coefficients of z^n.

From (4) we obtain, for $n \geqq 1$,

$$\overline{p_n(0)}p_n(z) = k_nz^n\bar{p}_n(z^{-1}) - k_{n-1}z^{n-1}\bar{p}_{n-1}(z^{-1}). \tag{7}$$

Proof. (i) Assuming that the same system $\{p_n(z)\}$ is orthogonal on a circle $|z| = R > 1$, we determine a sequence of positive numbers $\{\lambda_n\}$ such that $\{\lambda_n^{-1}p_n(Rz)\}$ is an orthonormal set, with a suitable weight function, on $|z| = 1$. Then, for $n \geqq 1$, we may write

$$\lambda_n^{-2}\overline{p_n(0)}p_n(Rz) = k_nR^n\lambda_n^{-2}z^n\bar{p}_n(Rz^{-1}) - k_{n-1}R^{n-1}\lambda_{n-1}^{-2}z^{n-1}\bar{p}_{n-1}(Rz^{-1}),$$

or

$$\lambda_n^{-2}\overline{p_n(0)}p_n(R^2z) = k_nR^{2n}\lambda_n^{-2}z^n\bar{p}_n(z^{-1}) - k_{n-1}R^{2n-2}\lambda_{n-1}^{-2}z^{n-1}\bar{p}_{n-1}(z^{-1}). \tag{8}$$

Eliminating $p_{n-1}(z)$ from (7) and (8), we obtain

$$\overline{p_n(0)}\left\{p_n(z) - R^{2-2n}\frac{\lambda_{n-1}^2}{\lambda_n^2}p_n(R^2z)\right\} = k_n\left\{1 - R^2\frac{\lambda_{n-1}^2}{\lambda_n^2}\right\}z^n\bar{p}_n(z^{-1}). \tag{9}$$

(ii) Let $n \geqq 2$, and $p_n(0) \neq 0$. If $1 - R^2\lambda_{n-1}^2/\lambda_n^2 = 0$, (9) shows that $p_n(z) = R^{-2n}p_n(R^2z)$; hence $p_n(z) = \text{const. } z^n$.

If $1 - R^2\lambda_{n-1}^2/\lambda_n^2 \neq 0$, and we set $p_n(z) = \sum_{\nu=0}^{n} c_\nu z_\nu$, we find from (9), for $\nu = 0, 1, 2, \cdots, n$, that

$$\overline{p_n(0)}c_\nu\left\{1 - R^{2-2n+2\nu}\frac{\lambda_{n-1}^2}{\lambda_n^2}\right\} = k_n\left\{1 - R^2\frac{\lambda_{n-1}^2}{\lambda_n^2}\right\}\bar{c}_{n-\nu},$$

and

$$p_n(0)\bar{c}_{n-\nu}\left\{1 - R^{2-2\nu}\frac{\lambda_{n-1}^2}{\lambda_n^2}\right\} = k_n\left\{1 - R^2\frac{\lambda_{n-1}^2}{\lambda_n^2}\right\}c_\nu.$$

Assuming $c_\nu \neq 0$, we have $c_{n-\nu} \neq 0$ and

$$|p_n(0)|^2\left\{1 - R^{2-2n+2\nu}\frac{\lambda_{n-1}^2}{\lambda_n^2}\right\}\left\{1 - R^{2-2\nu}\frac{\lambda_{n-1}^2}{\lambda_n^2}\right\} = k_n^2\left\{1 - R^2\frac{\lambda_{n-1}^2}{\lambda_n^2}\right\}^2, \tag{10}$$

which holds, in particular, for $\nu = 0$ and $\nu = n$. Using this equation, we see that the expression $R^{2-2n+2\nu} + R^{2-2\nu}$ is independent of ν. On the other hand, this expression is decreasing if ν increases from 0 to $n/2$. Consequently, (10) cannot hold unless $\nu = 0$ or $\nu = n$. Thus $p_n(z) = k_n z^n + l_n$. This result includes the case previously considered; in that case we have $l_n = 0$.

(iii) In both cases we obtain from (4) for $n \geqq 2$,

$$\sum_{\nu=0}^{n}\overline{p_\nu(0)}p_\nu(z) = \sum_{\nu=0}^{n-1}\overline{p_\nu(0)}p_\nu(z) + \bar{l}_n(k_nz^n + l_n) = k_n(\bar{l}_nz^n + k_n).$$

Hence $\sum_{\nu=0}^{n-1}\overline{p_\nu(0)}p_\nu(z) = \text{const.}$; that is,

$$p_1(0) = p_2(0) = \cdots = p_{n-1}(0) = 0.$$

As a consequence of this, it follows that $p_m(0) = 0$, $(m > n)$, and

$$k_mz^m\bar{p}_m(z^{-1}) = k_nz^n\bar{p}_n(z^{-1}).$$

Therefore, $k_m = k_n$, and we have the relation

$$p_m(z) = z^{m-n}p_n(z) = z^{m-n}(k_n z^n + l_n).$$

We have assumed, until now, that the sequence $p_2(0), p_3(0), \cdots$ contained a nonzero term. If this is not the case, the last result still holds with $n = 1$, as may be seen from (4) in the same way as before.

Now we have, if $m \geqq n$, $m' \geqq n$, $m \neq m'$,

$$\int_{-\pi}^{+\pi} f(\theta)e^{i(m-m')\theta} \left| k_n z^n + l_n \right|^2 d\theta = 0, \qquad z = e^{i\theta}.$$

Whence, except on a set of measure zero, we have

$$f(\theta) = \text{const.} \left| k_n z^n + l_n \right|^{-2}, \qquad z = e^{i\theta}. \tag{11}$$

We conclude the proof with the obvious remark that the polynomials $1, z, z^2, \cdots, z^{n-1}$ are orthogonal on the unit circle $|z| = 1$ with the weight function (11).

STANFORD UNIVERSITY

A FACTORIZATION THEOREM APPLIED TO A TEST FOR PRIMALITY*

D. H. LEHMER

Certain tests for primality based on the converse of Fermat's theorem and its generalizations have been devised and applied by the writer during the past ten years.† Perhaps the most useful test for the investigation of a large number N of no special form may be given as follows:‡

THEOREM 1. *If N divides $a^{N-1}-1$ but is relatively prime to $a^{(N-1)/p}-1$, where p is a prime, then all the possible factors of N are of the form $p^\alpha x+1$, if $N-1$ is divisible by p^α, $(\alpha \geqq 1)$.*

Strictly speaking this is not a test for primality since the theorem merely gives a restriction on the factors of N. If $p^\alpha > N^{1/2}$ then, obviously, N is a prime. If p^α is only fairly large, the theorem gives

* Presented to the Society, February 26, 1938.

† This Bulletin, vol. 33 (1927), pp. 327–340; vol. 34 (1928), pp. 54–56; vol. 35 (1929), pp. 349–350; vol. 38 (1932), pp. 383–384; vol. 39 (1933), pp. 105–108; Annals of Mathematics, (2), vol. 31 (1930), pp. 419–448; Journal of the London Mathematical Society, vol. 10 (1935), pp. 162–165; American Mathematical Monthly, vol. 43 (1936), pp. 347–354.

‡ This Bulletin, vol. 33 (1927), p. 331.